

UNITED STATES DISTRICT COURT

for the
District of New MexicoIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Samsung smartphone, serial number RF8K91Z1VKF,
currently stored at the FBI office located at 215 W Elm
St. Farmington, NM

Case No. 22-MR-1460

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ New Mexico _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 1153 &
2242(2)Offense Description
Sexual abuse committed in Indian Country

The application is based on these facts:

See attached affidavit, submitted by SA Nicole Montgomery and approved by AUSA Novaline Wilson

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Nicole Montgomery, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephonically sworn and electronically signed (specify reliable electronic means).

Date: September 30, 2022

City and state: Farmington, NM

Judge's signature

B. Paul Briones, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEW MEXICO

IN IN THE MATTER OF THE SEARCH OF:

- a. LG flip phone, model AX300SV, serial number 804CYWC0073425
- b. LG flip phone, model LG231C, serial number 107KPCA0183683
- c. Samsung flip phone, model SCH-R430, HEX: A000001498FE4A
- d. Samsung smartphone, model SM-J337A, serial number RF8K91Z1VKF, IMEI: 352146100121586

Case No. 22-MR-1460

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Nicole Montgomery, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property described in Attachment A—multiple electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. This affidavit in support of an application for a search warrant applies to electronic devices (referred to herein as the “TARGET DEVICES”) collected during the execution of United States District Court, District of New Mexico search warrant Case No. 22-MR-1383 at Navajo Housing Authority (“NHA”) House #5, Cudei, NM in vicinity of GPS coordinates 36.834931 -108.758468 on September 16, 2022.

2. I am “an investigative or law enforcement officer” of the United States within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

3. I am a Special Agent with the Federal Bureau of Investigation and have been employed as such since 2017. I am currently assigned to the Albuquerque Division, Farmington Resident Agency, which is responsible for investigating violent crimes occurring in Indian Country, including robbery, aggravated assaults, assaults on federal officers, sexual assaults, and homicides, as well as crimes involving children, including the production, distribution, and receipt of child pornography and kidnapping. I have eight years of prior law enforcement experience working as a police officer in the State of Illinois and as a detective in the Commonwealth of Virginia. Additionally, I attended three separate law enforcement academies and completed multiple in-service training courses relating to my duties.

4. I have received on the job training from other experienced agents and law enforcement officers. My investigative training and experience includes, but is not limited to, conducting surveillance, interviewing subjects, writing affidavits for search and arrest warrants, collecting evidence and learning legal matters which includes the topics of fourth amendment searches. I have experience executing and examining data from multiple search warrants on electronic devices and am familiar with the type of data stored on electronic devices. I have training and experience conducting investigations involving the use of electronic devices, websites, social media, and other forms of electronic communication, including the identification and use of IP addresses in determining user identities, geographic locations, and linked accounts.

5. The following information contained in this affidavit is based on my training and experience, my personal participation in this investigation, and information provided to me by other law enforcement officials. Unless otherwise indicated, where I have referred to written or oral statements, I have summarized them in substance and in part, rather than verbatim. Not all of the facts of the investigation known to me are contained herein, only those necessary to establish probable cause to search the below-listed items pertaining to the captioned investigation.

6. As will be shown below, there is probable cause to believe that the TARGET DEVICES will provide evidence of violations of 18 U.S.C. §§ 2242(2) and 1153 (Sexual Abuse in Indian Country) (hereinafter referred to as the “TARGET OFFENSES”). Based on the facts set forth in this affidavit, there is probable cause to believe that the TARGET OFFENSES were committed by Durward Deale, year of birth (YOB) 1980 (hereinafter referred to as “Deale”), an enrolled member of the Navajo Nation Indian Reservation, who resides at NHA House #5, Cudei, NM.

7. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence of the listed offenses is located in the TARGET DEVICES.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

8. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the TARGET DEVICES, which are currently in FBI possession, and the extraction from the TARGET DEVICES of electronically stored information described in Attachment B. This affidavit in

support of an application for a search warrant applies to the following TARGET DEVICES collected during the execution of United States District Court, District of New Mexico search warrant Case No. 22-MR-1383 at NHA House #5, Cudei, NM in vicinity of GPS coordinates 36.834931 -108.758468 on September 16, 2022:

- a. LG flip phone, model AX300SV, serial number 804CYWC0073425
- b. LG flip phone, model LG231C, serial number 107KPCA0183683
- c. Samsung flip phone, model SCH-R430, HEX: A000001498FE4A
- d. Samsung smartphone, model SM-J337A, serial number RF8K91Z1VKF,
IMEI: 352146100121586

9. The applied-for warrant would authorize the forensic examination of the TARGET DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Indian Country in the District of New Mexico. *See* 18 U.S.C. § 1153.

DEFINITIONS

11. The following terms are relevant to this affidavit in support of this application for a search warrant:

- a. *Computer*: The term “computer” refers to “an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, mobile phones, and devices. *See* 18 U.S.C. § 1030(e)(1).
- b. *Computer Hardware*: The term “computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- c. *Computer passwords and data security devices*: This term consists of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of

alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- d. *Electronic mail (“e-mail” or “email”)*: “E-mail” refers to a method of exchanging digital messages from an author to one or more recipients. Users may attach digital media to their e-mails. Modern e-mail operates across the Internet or other computer networks. E-mail systems are based on a store-and-forward model. E-mail servers accept, forward, deliver and store messages. E-mail accounts may be accessed by computers, to include smartphones and tablets.
- e. *File Transfer Protocol (“FTP”)*: FTP is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.
- f. *Hash Value*: A “hash value” is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file’s content. A hash value is a file’s “digital fingerprint” or “digital DNA.” Two files having identical content will have the same

hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

- g. *Internet*: The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- h. *Internet Protocol ("IP") Address*: An "IP address" is a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

- i. *Internet Service Providers (“ISPs”)*: “ISPs” are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.
- j. *Smartphone*: A “smartphone” is a type of mobile or cellular telephone, and functions as multi-purpose mobile-computing devices. Smartphones can function as traditional telephones with the additional ability to store contact information, send and receive voice, text, and media messages, store information and media, access the Internet, and perform many of the same functions as a traditional computer. A smartphone user may perform these various functions through software applications (“apps”) which may store evidence of such use on the device.
- k. *“Records,” “documents,” and “materials”*: These terms include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- l. *Visual Depictions*: “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

PROBABLE CAUSE

12. On September 13, 2022, the Sexual Assault Services (SAS) of New Mexico (NM) contacted the FBI regarding the sexual assault of C.N., YOB 1985 (hereinafter referred to as “Jane Doe,” an enrolled member of the Navajo Nation), on September 11, 2022. Jane Doe alleged that her ex-common law husband, Deale, sexually assaulted her in her sleep in their shared residence, located at NHA House #7, Newcomb, NM (GPS coordinates 36.284013,-108.707237), which is located within the exterior boundaries of the Navajo Nation Indian Reservation. Jane Doe was interviewed by the FBI on September 13, 2022.

13. According to Jane Doe, she and Deale began a dating relationship in 2005 and dated on and off until 2012. Deale was mentally and emotionally abusive toward Jane Doe in the beginning, and it eventually escalated to physical violence. During their relationship, Deale would secretly photograph and video record them having consensual sex. Jane Doe only discovered he was doing this after looking through his phone and finding photographs and videos. She would also catch Deale watching pornography on his phone while having sex with her. Jane Doe believed Deale had an addiction to pornography, as she would find “jump” drives containing numerous pornographic images, meticulously organized by year and porn star. She and Deale would argue about his pornography collection, and it would often lead to them breaking up, only to later get back together.

14. Jane Doe and Deale had two children together and filed paperwork with the Navajo Nation to become married via common law. Anytime Jane Doe and Deale separated, he would take the children from Jane Doe. They separated in 2017 after Jane Doe found the “jump” drives containing pornography. In 2019, Jane Doe was approved for NHA housing and moved into her house in Newcomb. She asked Deale if the children could move in with her. Deale

agreed, but only if he could move in, as well. Jane Doe had her own bedroom and Deale would sleep in the living room on the couch. They attempted throughout the years to reconcile, but it never lasted. Deale continued to live with Jane Doe and their children, but for the past six months, Jane Doe has not consented to sex with Deale.

15. On May 16, 2022, Jane Doe woke up with pain in her vagina, feeling like she had sex. On May 17, she woke up again feeling like she had sex, with accompanied bleeding from her vagina. On May 18, she woke up and used the bathroom. She had pain when she urinated, and upon further inspection, located a scratch on her vagina. On May 19, she awoke again feeling like something happened to her. Jane Doe was not sexually active with anyone during this time period and had not been sexually active with Deale for several months.

16. On May 20, 2022, Jane Doe, Deale, and their two children went to Pizza Hut in Farmington, NM to pick up dinner. While waiting, their son was playing on Deale's unlocked iPhone. When Deale went inside to get the pizza, Jane Doe took the opportunity to look in Deale's phone. She found photographs and a video of her naked body. In the video and images, Jane Doe was lying face down, naked on her bed. The video showed a hand touching Jane Doe's buttocks. Jane Doe identified her body and recognized Deale's hand in the video. The photographs showed object placed on her buttocks, such as two plush toys belonging to the children. Other photographs showed Jane Doe wearing a thong that she did not put on prior to going to sleep. Jane Doe confronted Deale about the contents of his phone. He told her the images she saw were from the fifth time he touched her in her sleep, and that he had done it to her four times prior. According to Jane Doe, she has always been a heavy sleeper, and she would take melatonin, which would put her into an even deeper sleep.

17. On July 17, 2022, Jane Doe returned home from a camping trip. She drank alcohol at home before going to sleep alone in her bed. The next morning, she woke up and used the bathroom. Her vagina hurt and it felt like she had sex the night prior. She looked down at her underwear and saw she was wearing a backwards thong. She had gone to sleep in a different pair of underwear. When she confronted Deale about it, he told her that he was rubbing her feet and she smelled like urine so he changed her underwear. Jane Doe questioned why he changed her underwear and not her shorts, if she truly peed on herself. On July 20, 2022, Jane Doe began bleeding from her vagina again. She took a photograph of the bloody toilet paper and confronted Deale with it, as she is on birth control and no longer gets periods. In a text message exchange, Deale denied having sex with her, but said, "I rubbed your lower body all."

18. Approximately one month ago, around the beginning of August 2022, Jane Doe went through her daughter's Apple iPad to make sure she was not doing anything inappropriate. In the photos folder, she found and viewed a video of Deale touching her (Jane Doe). It is unknown whether the video was taken with the camera on iPad, or if the video was transferred from the iPad from a different device.

19. On September 11, 2022, Jane Doe, Deale, and their family had dinner together. Jane Doe and Deale consumed alcohol. Jane Doe drank approximately three mixed drinks and two glasses of wine. Just before 9:00 p.m., she went to sleep in her bedroom with her juvenile son. Deale followed her to her room to rub her feet, as she suffers from foot issues. Foot massages are not considered sexual foreplay for Jane Doe and Deale and has never led to sex. Jane Doe fell asleep on her stomach while Deale rubbed her feet.

20. Jane Doe, still in a drowsy state after being asleep and consuming alcohol, felt movement on the bed. Her son was no longer in the room. As she lay on the bed, Jane Doe felt

Deale put liquid on her vagina, insert his finger into her vagina, and then insert his penis two times into her vagina. She also saw a flash, as if a photograph or video was taken of her. He then pulled off a thong that Jane Doe was not previously wearing. He wiped her vagina with a baby wipe and lied down on the bed next to her abruptly since Jane Doe started to move. Jane Doe described that these events transpired quickly. Jane Doe, now fully alert, mounted Deale, choked him, and threatened to kill him if he ever touched her again. They continued to verbally argue, with Deale telling her that she “set him up.” Jane Doe kicked him out of her bedroom after they stopped arguing. She text messaged him at 12:40 a.m. telling him it was not okay for him to rape her and that he could not stay at her house anymore. Deale did not respond.

21. The next morning, Jane Doe found the white thong, baby oil, baby wipes, and Deale’s cell phone in her bedroom. She photographed most of the objects. Jane Doe had a sexual assault examination later that day in Gallup, NM. After returning home, she discovered Deale had cleaned her bedroom, either hiding or taking with him the baby oil and white thong. He and the children went to Deale’s parents’ house (the SUBJECT PREMISES), located at NHA House #5, Cudei, NM (GPS coordinates 36.834931,-108.758468). Whenever Deale is not staying with Jane Doe at her house in Newcomb, NM, he stays at the SUBJECT PREMISES, as he does not work and does not have the financial means to rent his own house or apartment.

22. On September 16, 2022, FBI Agents of the Farmington Resident Agency, in conjunction with other law enforcement partners, executed search warrant 22-MR-1383, issued in United States District Court, District of New Mexico, at NHA House #5, Cudei, NM. The search warrant included the search of Deale’s blue Chevrolet Malibu, bearing New Mexico license plate 366TWT and vehicle identification number (“VIN”) 1G1ZC5E19BF271578, which was parked in the residence driveway at the time of the search.

23. When law enforcement officers attempted to gain entry to the Malibu, Deale stated he never drives the vehicle. According to Jane Doe, Deale drives their children to school in the Malibu and it was driven from Newcomb to Cudei on September 12, 2022 after Jane Doe kicked him out of her house. While law enforcement officers were searching the Malibu, Deale's mother, who was present during the search, attempted to gain entry to the vehicle and remove items before officers could locate them. When she was asked what she was looking for, she said that there were three cell phones in the vehicle. Additionally, Deale told a law enforcement officer on scene that there was a bag containing three cell phones inside the vehicle. The TARGET DEVICES were seized from the residence and Deale's Malibu.

24. Deale told a law enforcement officer that there would be hundreds of pornographic photographs and videos on his cell phones, in addition to graphic photographs of he and Jane Doe having consensual sex. Deale said he would photograph them having sex and continue photographing Jane Doe after she passed out. While informing Deale of the devices seized, Deale stated there would be photos of "her" on the turquoise cell phone (identified as TARGET DEVICE "c"), which were the first photos that started his "fetish thing." Deale also told law enforcement officers that he had an addiction to pornography and that it affected his ability to get an erection when Jane Doe did want to have consensual sexual relations with him.

25. During the execution of the search warrant, Deale's daughter's iPad, believed to be in Deale's possession, was not located. On September 19, 2022, Jane Doe notified law enforcement that the iPad was located in her house in Newcomb. Jane Doe examined the iPad and discovered the video of herself she previously located was now gone and the "Recently Deleted" folder was empty.

26. Based on my training, experience, and research from consulting the manufacturer's advertisements and product technical specifications, I know that the TARGET DEVICES have capabilities that allow them to serve as a wireless telephone, digital camera, GPS navigation device, and is capable of connecting to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, where the user was located at specific times, and communications between different parties over various communication platforms.

27. Additionally based on my training, experience, and research from consulting the manufacturer's advertisements and product technical specifications, I know that the TARGET DEVICES have capabilities that allow them to be used as both digital cameras, as well as storage devices for images, photographs, and other media. The TARGET DEVICES are capable of accepting the transfer of images, photographs, and other media from other computers

BACKGROUND ON COMPUTERS AND THE INTERNET

28. I have both training and experience in the investigation of computer-related crimes. Based on my training and knowledge, I know the following:

- a. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs and/or videos.

- b. A device known as a “modem” allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections.
- c. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices, which plug into a port on a computer or tablet, either directly or through the use of an external disc drive or port adapter – can store thousands of images and/or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer or tablet, and then copy it (or any other files on the computer or tablet) to any one of those media storage devices.
- d. Individuals also use online resources to retrieve and store photographic evidence. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find photographic evidence on the user’s computer, smartphone or external media in most cases.

OFFENDER CHARACTERISTICS

29. Based on my previous investigative experience related to sexual assault investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who create and/or possess photographic evidence of their crimes:

- a. Such individuals may receive sexual gratification, stimulation (including erectile function), and satisfaction from having sexual contact with persons who are unable to consent to the sexual contact, or from fantasies they have viewing non-consenting persons in sexually suggestive poses, such as in person or in photographs.
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media.
- c. Such individuals often maintain their pornography material in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. This pornography material is often maintained for several years and kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the pornography images at leisure.
- d. Importantly, evidence of such activity, including deleted pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic

storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.

- e. Such individuals often transfer electronic files containing pornography from device to device, either to make room on their devices, or for long-term storage.

30. I also know from training and experience that some persons who create and/or possess pornography or photographic evidence of their sexual crimes engage in “collector behavior.” Persons who are “collectors” of pornography or photographic evidence of their sexual crimes often keep the material in their possession for years, because it is considered valuable to them. They may receive sexual gratification, stimulation (including erectile function), and satisfaction from reviewing the photographs and videos they created. “Collectors,” in an attempt to prevent their valuable images from being lost, stolen, damaged, or corrupted, will often transfer images to other devices capable of media storage, and may store their images on multiple devices. They may also remove the images from the devices they use on a daily basis to other devices, such as computers, cell phones, or other external storage devices, to avoid the images being seen by others. “Collectors” rarely permanently delete their collection of illicit photographs, videos, and images.

31. Given Deale’s history of downloading, saving, and cataloging pornographic images retrieved from the Internet to external devices, such as jump drives, and his admission of keeping hundreds of images of Jane Doe on his old cell phones for years and travelling from residence to residence with them, I believe he exhibits “collector” behavior. Additionally, it is reasonable to believe that since the video of Jane Doe from her daughter’s iPad is now gone from the device, that it was merely removed from that device and transferred to another.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a

dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

36. Based on the facts set forth in this affidavit, there is probable cause to believe violations of Title 18 U.S.C. §§ 2242(2) and 1153 (Sexual Abuse in Indian Country) were

committed by Deale and that evidence, contraband, instrumentalities and/or fruits of violations of such crimes may be contained in the TARGET DEVICES.

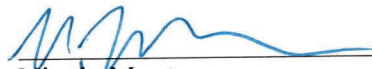
37. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

38. Given that the TARGET DEVICES are contained on the premises of the FBI, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

39. Assistant United States Attorney Novaline D. Wilson reviewed this affidavit for legal sufficiency.

40. I swear that this information is true and correct to the best of my knowledge and belief.

Respectfully submitted,



Nicole Montgomery
Special Agent
Federal Bureau of Investigation

Telephonically sworn and electronically signed on this 30th day of September 2022.



B. Paul Briones
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched include the following electronic devices which were collected during the execution of United States District Court, District of New Mexico search warrant Case No. 22-MR-1383 at Navajo Housing Authority (“NHA”) House #5, Cudei, NM in vicinity of GPS coordinates 36.834931 -108.758468 on September 16, 2022, which are currently in FBI custody stored at the FBI Office located at 215 W Elm St, Farmington, NM:

- a. LG flip phone, model AX300SV, serial number 804CYWC0073425
- b. LG flip phone, model LG231C, serial number 107KPCA0183683
- c. Samsung flip phone, model SCH-R430, HEX: A000001498FE4A
- d. Samsung smartphone, model SM-J337A, serial number RF8K91Z1VKF,
IMEI: 352146100121586

This warrant authorizes the forensic examination of the Target Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records, in whatever format, on the TARGET DEVICES described in Attachment A that relate to violations of United States Code Title 18 U.S.C. §§ 2242(2) and 1153 (Sexual Abuse in Indian Country) that involve Deale and are related to content regarding Jane Doe for the time period of May 15, 2022 to September 16, 2022 including:

- a. Digital, cellular, direct connect, and/or other phone numbers, names, addresses, and other identifying information;
- b. Digital, cellular, direct connect, and/or other phone numbers dialed from, which contacted, or which are otherwise stored on, the TARGET DEVICES, along with the date and time each such communication occurred;
- c. Text message logs and text messages whether sent from, to, or drafted on, the TARGET DEVICES, along with the date and time each such communication occurred;
- d. The content of voice mail messages stored on the TARGET DEVICES, along with the date and time each such communication occurred;
- e. Photographs or video recordings;
- f. Information relating to other methods of communications utilized by the user of the TARGET DEVICES and stored on the TARGET DEVICES;

- g. Evidence of user attribution showing who used or owned the TARGET DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history, and;
- h. The content of any communication in whatever format between the user of the TARGET DEVICES and Jane Doe, along with the date and time each such communication occurred.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.